KAREN STEPHENS

Karen Stephens is theco-founder and CEO of BCyber. After more than 25 years in financial services, Karen moved into SME cybersecurity risk management. She works with SMEs to protect and grow their businesses by demystifying the technical aspects of cybersecurity and helping them to identify and address cybersecurity and governance risk gaps. She was recently named inaugural Female Cyber Leader of the Year at the 2023 CyberSecurity Connect Awards in Canberra.

COLUMN

Are we there yet?

Are we there yet? If you are asking this question in relation to Australian companies' cyber resilience, the answer is no, not by a long shot. Don't believe me. Believe the Australian Signals Directorate (ASD) whose most recent Cyber Threat Report shows the ASD receiving a cybercrime notification every six minutes, and fielding an average of 100 hotline calls each day.

Those statistics tell us quite clearly that nefarious cyber activity is still rampant and that cybersecurity is not done and dusted, it is a journey. In fact, it is a never-ending journey, and there is no crib sheet. If the recent FIIG Securities (FIIG) case tells us anything it's that "Cybersecurity isn't a set and forget matter. All companies need to proactively and regularly check the adequacy of their cybersecurity measure."

Let's debunk three cyber myths and help you in your quest for a cyber safe life.

1. **Cyber is just a tech problem.** No. The involvement of the human element in breaches is hovering around 60 percent. The bottom line is you can have the best security software in the world, but if you or a colleague insists on clicking on every link known to mankind, then your security software must be 100 percent secure 100 percent of the time, and we know that is unrealistic.
2. **Cyber criminals are 'lone wolves' in someone's basement.** No. Cybercrime is a business, a very, very big business. If cyber criminals were a country they would be the world's third largest economy behind the USA and China.
3. **We use all the web.** No. People typically engage with only the so-called visible web, ie the section that houses websites and whose content is indexed by standard search engines (eg Google, Edge etc). It accounts for about four percent of what is available. The remaining 96 percent is made up of the deep web and the dark web.

It's not all doom and gloom. Here are three no-cost strategies to enhance both your personal and your company's cyber resilience.

1. **Good password hygiene.** While it may not be glamorous, maintaining strong passwords can prevent numerous problems. Aim for at least 16 complex characters. Never reuse or share passwords and consider using a password manager.
2. **Trust no one, verify everything.** If you receive a call from an unknown number, let it go to voice mail. If you receive a great offer via email, delete it and go straight to the website of the source. There are many more examples, but I think you get the gist.
3. **Treat your mobile with respect.** These days mobile phones are mini supercomputers. In fact the iPhone in your pocket has over 100,000 times the processing power of the computer that landed man on the moon 50 years ago. Ensure your device's hardware, software and apps are up to date. Take some time to remove any unnecessary apps and delete any you do not use.

So, are we there yet? No, but hopefully we've cleared up some misconceptions and fortified both your personal and company cybersecurity practices.

www.linkedin.com/in/karen-stephens-bcyber

www.bcyber.com.au *x.com/bcyber2*

karen@bcyber.com.au *youtube.bcyber.com.au/2mux*